

(19)



Europäisches Patentamt

European Patent Office

Office européen des brevets



(11)

EP 0 811 739 A2

(12)

EUROPÄISCHE PATENTANMELDUNG

(43) Veröffentlichungstag:
10.12.1997 Patentblatt 1997/50

(51) Int. Cl.⁶: E05B 49/00, B60R 25/04

(21) Anmeldenummer: 97108985.9

(22) Anmeldetag: 04.06.1997

(84) Benannte Vertragsstaaten:
AT BE CH DE DK ES FI FR GB GR IE IT LI LU MC
NL PT SE

(30) Priorität: 06.06.1996 DE 19622721

(71) Anmelder:
F + G Megamos Sicherheitselektronik GMBH
51674 Wiehl (DE)

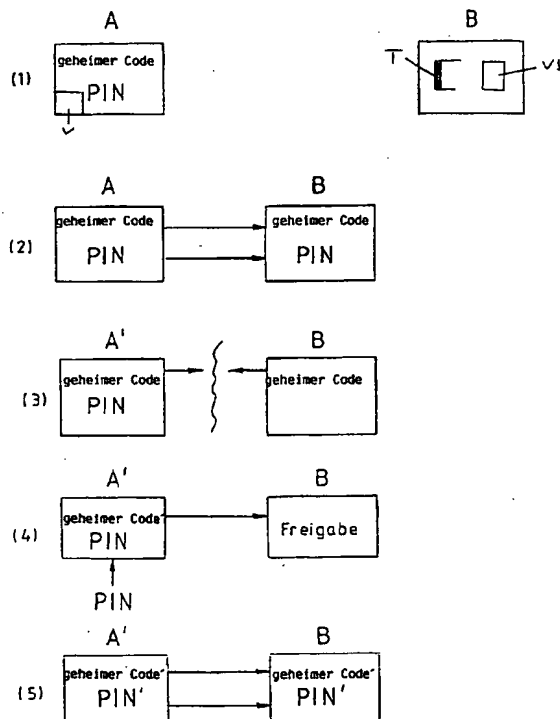
(72) Erfinder:
• Konrad, Reimund
51647 Gummersbach (DE)
• Petsching, Wilfried
51688 Wipperfürth (DE)
• Weiss, Bernd
51647 Gummersbach (DE)

(74) Vertreter: Cohausz & Florack
Patentanwälte
Kanzlerstrasse 8a
40472 Düsseldorf (DE)

(54) **Vorrichtung und Verfahren zur Prüfung der Nutzungsberechtigung für Zugangskontrolleinrichtungen, insbesondere Schliesseinrichtungen für Fahrzeuge**

(57) Die Erfindung betrifft eine Vorrichtung und ein Verfahren zur Prüfung der Nutzungsberechtigung für Zugangskontrolleinrichtungen, insbesondere Schließ-einrichtungen für Fahrzeuge. Um eine Verwendung derselben Schlüsseinrichtung auch beim Austausch des Steuergerätes (A) gegen ein anderes Steuergerät (A') verwenden zu können, sieht die Erfindung vor,

- a) daß Speichermittel einer zugangsseitigen Steuereinrichtung (A) einen geheimen Code (secret key) und einen Benutzercode (PIN) speichern,
- b) daß in dem Transponder (T) einer benutzerseitigen Schlüsseinrichtung (B) der geheime Code (secret key) und der Benutzercode (PIN) durch Anlernen von der Steuereinrichtung (A) niedergelegt sind,
- c) daß die vom Transponder (T) ausgesandte Information, aus einer nach dem angelernten geheimen Code verschlüsselten Benutzercodeinformation besteht,
- d) und daß die Schlüsseinrichtung (B) weitere Vergleichsmittel (Vb) umfaßt, die mit Verriegelungsmitteln (Lockbits) für den geheimen Code (secret key) derart gekoppelt sind, daß mindestens eine teilweise Freigabe zum Überschreiben des in der Schlüsseinrichtung gespeicherten geheimen Codes (secret key) erfolgt, wenn die weiteren Vergleichsmittel (Vb) eine Übereinstimmung des von der Steuereinrichtung ausgesandten Benutzercode (PIN) mit dem abgespeicherten Benutzercode (PIN) feststellen.



EP 0 811 739 A2

Beschreibung

Die Erfindung betrifft eine Vorrichtung bzw. ein Verfahren zur Prüfung der Nutzungsberechtigung für Zugangskontrolleinrichtungen, insbesondere Schließ-

einrichtungen für Fahrzeuge.
Bei einer solchen Vorrichtung bzw. bei einem solchen Verfahren erfolgt ein Austausch von Identifikationsdaten zwischen einem zugangsseitigen dauerenergieversorgten Steuergerät, welches sich beispielsweise im Fahrzeug befindet, und einer benutzerseitigen Schlüsseleinrichtung, beispielsweise einem Fahrzeugschlüssel. Die Schlüsseleinrichtung enthält dabei einen Transponder, welcher bei elektromagnetischer Anregung durch Signale des Steuergerätes angeregt eine Signalfolge aussendet, die wiederum im Steuergerät empfangen wird.

Zur Feststellung der Zugangsberechtigung wird in dem Steuergerät überprüft, ob die von der Schlüsseleinrichtung empfangene Signalfolge aus einem autorisierten Schlüssel stammt. Hierzu wird ausgehend von einem Initialzustand, bei dem im Transponder kein Verschlüsselungscode hinterlegt wird, dort ein geheimer Code von demjenigen Steuergerät angelernt, für das die Schlüsseleinrichtung dienen soll. Der geheime Code in der Schlüsseleinrichtung entspricht dann dem geheimen Code des verwendeten Steuergerätes. Sämtliche für das Fahrzeug geltenden Schlüssel werden auf diese Weise an den geheimen Code des Steuergerätes angelernt. Der geheime Code ist als solcher nicht lesbar. Er dient dazu, die von der Schlüsseleinrichtung empfangene Information zu codieren, so daß das Steuergerät aus der rückübertragenen Information von der Schlüsseleinrichtung erkennt, daß diese einem autorisierten Schlüssel zugeordnet ist.

Solche Vorrichtungen sind beispielsweise aus der DE 4317119 C2 und der DE 4435894 A1 bekannt.

Dadurch, daß der geheime Code der Schlüsseleinrichtung selber nicht lesbar ist, können die an ein bestimmtes Steuergerät angelernten Schlüssel beim Ausfall dieses Steuergerätes üblicherweise nicht mehr weiter verwendet werden.

Der Erfindung liegt davon ausgehend die Aufgabe zugrunde, ein Verfahren bzw. eine Vorrichtung der eingangs genannten Art dahingehend weiterzuentwickeln, daß auch nach dem Ersatz des Steuergerätes durch ein weiteres Steuergerät die vorhandenen Schlüsseleinrichtungen weiter verwendet werden können.

Diese Aufgabe wird bei einer Vorrichtung zur Prüfung der Nutzungsberechtigung für Zugangskontrolleinrichtungen, die

- eine zugangsseitige Steuereinrichtung mit Speichermitteln für einen Code,
- eine benutzerseitige Schlüsseleinrichtung, die einen Transponder enthält, sowie
- Vergleichsmittel in der Steuereinrichtung zur Feststellung der für die Freigabe der Zugangsein-

richtung erforderlichen Berechtigung, derart, daß die vom Transponder ausgesandte Information mit einer in der Steuereinrichtung festgelegten Vorgabeinformation verglichen wird und daß nur bei einer Übereinstimmung eine Freigabe des Zugangs erfolgt,

umfaßt, dadurch gelöst,

- a) daß die Speichermittel der zugangsseitigen Steuereinrichtung einen geheimen Code (secret key) und einen Benutzercode (PIN) speichern,
- b) daß in dem Transponder der benutzerseitigen Schlüsseleinrichtung der geheime Code (secret key) und der Benutzercode (PIN) durch Anlernen, insbesondere von der Steuereinrichtung, niedergelegt sind,
- c) daß die vom Transponder ausgesandte Information, die von dem Vergleichsmitteln in der Steuereinrichtung zur Feststellung der für die Freigabe der Zugangseinrichtung erforderlichen Berechtigung mit der in der Steuereinrichtung festgelegten Vorgabeinformation verglichen wird, aus einer nach dem angelernten geheimen Code verschlüsselten Benutzercodeinformation besteht,
- d) daß die Schlüsseleinrichtung weitere Vergleichsmittel umfaßt, die mit Verriegelungsmitteln (Lock-bits) für den geheimen Code (secret key) derart gekoppelt sind, daß mindestens eine teilweise Freigabe zum Überschreiben des in der Schlüsseleinrichtung gespeicherten geheimen Codes (secret key) erfolgt, wenn die weiteren Vergleichsmittel (Vb) eine Übereinstimmung des von der Steuereinrichtung ausgesandten Benutzercode (PIN) mit dem abgespeicherten Benutzercode (PIN) feststellen.

Bei einem Verfahren zur Prüfung der Nutzungsberechtigung für Zugangskontrolleinrichtungen, bei dem zwischen einem zugangsseitigen, dauerenergieversorgten Steuergerät und einer benutzerseitigen einen Transponder enthaltenden Schlüsseleinrichtung bidirektional Identifikationsdaten ausgetauscht werden, wobei die Feststellung der für die Freigabe der Zugangseinrichtung erforderlichen Berechtigung derart erfolgt, daß eine vom Transponder ausgesandte Codeinformation mit einer in der Steuereinrichtung festgelegten Vorgabeinformation verglichen wird und daß nur bei einer Übereinstimmung eine Freigabe des Zugangs erfolgt, wird diese Aufgabe dadurch gelöst, daß

- a) zunächst die Schlüsseleinrichtung an einen im Steuergerät abgelegten geheimen Code (secret key) sowie einen Benutzercode (PIN) angelernt wird, und anschließend die vom Transponder ausgesandte Information für den Vergleich mit der in der Steuereinrichtung festgelegten Vorgabeinformation zur Feststellung der für die Freigabe der

Zugangseinrichtung erforderlichen Berechtigung nach dem angelernten geheimen Code verschlüsselt wird, und

b) beim Ersetzen des Steuergerätes durch ein weiteres Steuergerät zunächst der Benutzercode (PIN) des ersten Steuergerätes zur Schlüsseleinrichtung übertragen wird, wodurch in der Schlüsseleinrichtung nach Prüfung der Übereinstimmung des empfangenen Benutzercodes (PIN) mit dem angelernten Benutzercode (PIN) der geheime Code mindestens teilweise zum Überschreiben freigegeben wird, und daß anschließend durch Übertragen des für das weitere Steuergerät geltenden geheimen Codes (secret key) die Schlüsseleinrichtung an den für das weitere Steuergerät geltenden geheimen Code angelernt wird.

Die Erfindung zeichnet sich dadurch aus, daß beim Ausfall eines Steuergerätes dessen alte PIN-Nummer in das neue (weitere) Steuergerät eingegeben wird und hierdurch der Bereich des geheimen Codes in der Schlüsseleinrichtung bei Übereinstimmung mit dem in der Schlüsseleinrichtung hinterlegten, von dem ursprünglichen Steuergerät angelernten Benutzercode (PIN) freigegeben wird. Nach dessen Freigabe kann er mit dem neuen geheimen Code und dem neuen Benutzercode des neuen Steuergerätes überschrieben werden, so daß dieselbe Schlüsseleinrichtung im Anschluß daran für das neue Steuergerät autorisiert ist. Somit kann unter Beibehaltung des für die Sicherheit wesentlichen Vorteils, daß der geheime Code in der Schlüsseleinrichtung nicht lesbar ist, gleichwohl der Vorteil der Anpaßbarkeit derselben Schlüsseleinrichtung an ein Ersatz-/ Steuergerät erreicht werden.

Bevorzugte Ausführungsformen gehen aus den Unteransprüchen hervor.

Dabei ist es von besonderer Bedeutung, daß die erfindungsgemäße Vorrichtung gegen Manipulation dadurch geschützt ist, daß nur eine begrenzte Anzahl von Übertragungsvorgängen des Benutzercodes PIN zulässig ist. Falls nämlich - wie dies bei vergleichbaren Code-Sicherungen, wie beispielsweise beim Mobiltelefon oder bei Geldautomaten bekannt ist - mehrfach ein falscher Benutzercode eingegeben wurde, wird die Verriegelung des geheimen Codes in der Schlüsseleinrichtung blockiert, so daß keinesfalls ein Überschreiben des geheimen Codes mehr möglich ist.

Die Erfindung wird im folgenden anhand eines Ausführungsbeispiels näher erläutert. Hierzu wird auf die Erläuterungsskizze Bezug genommen.

Mit dem Bezugszeichen A ist ein zugangsseitiges, insbesondere dauerenergieversorgtes Steuergerät bezeichnet und mit B eine benutzerseitige Schlüsseleinrichtung.

Zunächst befinden sich in dem Steuergerät A ein geheimer Code (secret key) sowie ein Benutzercode (PIN), der werkseitig einprogrammiert wurde. Nur der Benutzercode ist dem Fahrzeugbesitzer bekannt. Die

Schlüsseleinrichtung B befindet sich demgegenüber im Initialzustand, in dem keine Codierung innerhalb des in der Schlüsseleinrichtung angeordneten Transponders vorliegt. Im Schritt 2 wird die Schlüsseleinrichtung B sowohl an den geheimen Code (secret key) als auch an den Benutzercode PIN des Steuergerätes A angelernt, indem die entsprechenden Codes in den secret-key-Bereich des Transponders in der Schlüsseleinrichtung B übertragen werden. Hierzu weist der secret-key-Bereich des Transponders eine Länge von 95 Bit auf, wobei Bit 0 bis Bit 15 schlüsselspezifisch und Bit 16 bis Bit 95 fahrzeugspezifisch vorgebar sind. Im Bereich von Bit 80 bis Bit 95 wird der Benutzercode PIN des Steuergerätes des Fahrzeuges hinterlegt.

Nach diesem Vorgang ist der geheime Code innerhalb der Schlüsseleinrichtung derart abgespeichert, daß er in keinem Fall lesbar ist. Er ist über Lockbits dahingehend verriegelt, daß er nur dann, wenn eine entsprechend dem Benutzercode PIN eingegebene Zahlenfolge identifiziert wird, zum Überschreiben mit einem anderen geheimen Code freigegeben wird.

Dieser Vorgang nach Stufe 2 wird für alle Schlüsseleinrichtungen wiederholt, die mit dem Steuergerät A in Verbindung stehen sollen.

In Stufe 3 ist nun angenommen, daß das bisherige Steuergerät A ausgefallen ist und durch ein neues Steuergerät A' ersetzt werden soll, welches werkseitig einen anderen geheimen Code secret key' sowie einen abweichenden Benutzercode PIN' aufweist. Hierdurch ist zunächst eine Benutzung der auf das ursprüngliche Steuergerät A angelernten Schlüsseleinrichtung B ausgeschlossen, da keine Übereinstimmung in den secret key's vorliegt.

Daher erfolgt gemäß Schritt 4 die Eingabe des ursprünglichen PIN-Codes (des alten Steuergerätes A) in das neue Steuergerät A'. Die Eingabe erfolgt beispielsweise mittels eines Diagnose-Testers. Durch die Übertragung der alten PIN-Nummer zum Transponder wird der Schlüsseleinrichtung mitgeteilt, daß dieser in den "Replace Mode" gehen soll, dies bedeutet, daß der Bereich des geheimen Codes innerhalb des Transponders durch entsprechend gesetzte Lockbits beschreibbar wird. Hierdurch wird der Bereich des secret key in der Schlüsseleinrichtung zum Überschreiben mit dem neuen secret key' des neuen Steuergerätes A' sowie der neuen PIN-Nummer PIN' freigegeben. Hierdurch wird die Schlüsseleinrichtung B anwendbar für das neue Steuergerät A'.

Die beschriebenen Vorgänge werden nacheinander auf sämtliche vorhandenen Schlüsseleinrichtungen angewendet, so daß schließlich alle ursprünglichen Schlüsseleinrichtungen auch für das neue Steuergerät A' verwendbar sind.

Somit kann der Fahrzeugbesitzer auch im Falle eines notwendigen Austausches des Steuergerätes die ihm beim Fahrzeugkauf übergebenen Schlüssel weiter benutzen.

Der beschriebene Vorgang weist noch einen in der

Zeichnung nicht dargestellten Sicherheitsaspekt auf, der darin besteht, daß ein Zähler für die Anzahl der Übertragungsvorgänge des PIN-Codes in der Schlüsseleinrichtung vorhanden ist. Jedes Mal, wenn der Replace Mode ausgeführt wird, d.h. ein PIN-Code zum Transponder gesendet wird, wird dieser von außen nicht beschreibbare Zähler um eins erhöht. Der Zähler weist darüber hinaus die Vorgabemöglichkeit eines Grenzwertes auf, beispielsweise der Zahl Zehn. Dies hat zur Folge, daß die Verriegelung des geheimen Codes blockiert wird, falls zehn Eingaben von PIN-Codes erfolgt sind und zuvor noch keine Freigabe der Lockbits zum Überschreiben des geheimen Codes erfolgt ist. Hierdurch wird verhindert, daß beispielsweise sämtliche möglichen PIN-Codes der Reihe nach eingegeben (eingescannt) werden und hierdurch der Schlüssel in den ursprünglichen Zustand versetzt werden und somit unbrauchbar würde.

Patentansprüche

1. Vorrichtung zur Prüfung der Nutzungsberechtigung für Zugangskontrolleinrichtungen, insbesondere Schließeinrichtungen für Fahrzeuge, mit

- einer zugangsseitigen Steuereinrichtung (A) mit Speichermitteln für einen Code,
- einer benutzerseitigen Schlüsseleinrichtung (B), die einen Transponder (T) enthält, sowie
- Vergleichsmitteln (V) in der Steuereinrichtung (A) zur Feststellung der für die Freigabe der Zugangseinrichtung erforderlichen Berechtigung, derart, daß die vom Transponder (T) ausgesandte Information mit einer in der Steuereinrichtung (A) festgelegten Vorgabeinformation verglichen wird und daß nur bei einer Übereinstimmung eine Freigabe des Zugangs erfolgt,

dadurch gekennzeichnet,

- a) daß die Speichermittel der Zugangsseitigen Steuereinrichtung (A) einen geheimen Code (secret key) und einen Benutzercode (PIN) speichern,
- b) daß in dem Transponder (T) der benutzerseitigen Schlüsseleinrichtung (B) der geheime Code (secret key) und der Benutzercode (PIN) durch Anlernen, insbesondere von der Steuereinrichtung (A), niedergelegt sind,
- c) daß die vom Transponder (T) ausgesandte Information, die von dem Vergleichsmitteln (V) in der Steuereinrichtung (A) zur Feststellung der für die Freigabe der Zugangseinrichtung erforderlichen Berechtigung mit der in der Steuereinrichtung (A) festgelegten Vorgabeinformation verglichen wird, aus einer nach dem angelernten geheimen Code verschlüsselten

Benutzercodeinformation besteht,

d) und daß die Schlüsseleinrichtung (B) weitere Vergleichsmittel (Vb) umfaßt, die mit Verriegelungsmitteln (Lockbits) für den geheimen Code (secret key) derart gekoppelt sind, daß mindestens eine teilweise Freigabe zum Überschreiben des in der Schlüsseleinrichtung gespeicherten geheimen Codes (secret key) erfolgt, wenn die weiteren Vergleichsmittel (Vb) eine Übereinstimmung des von der Steuereinrichtung ausgesandten Benutzercode (PIN) mit dem abgespeicherten Benutzercode (PIN) feststellen.

2. Vorrichtung nach Anspruch 1

dadurch gekennzeichnet, daß die Schlüsseleinrichtung einen zusätzlichen Zähler aufweist für die Anzahl der Übertragungsvorgänge des Benutzercodes (PIN) vom Steuergerät auf die Schlüsseleinrichtung.

3. Vorrichtung nach Anspruch 2,

dadurch gekennzeichnet, daß dem zusätzlichen Zähler ein Grenzwert vorgebar ist, bei dessen Erreichen die Freigabe der Verriegelungsmittel blockiert wird.

4. Vorrichtung nach einem der vorhergehenden Ansprüche,

dadurch gekennzeichnet, daß der geheime Code aus mehreren Abschnitten besteht.

5. Vorrichtung nach Anspruch 4

dadurch gekennzeichnet, daß einer der Abschnitte schlüsselspezifisch und ein anderer fahrzeugspezifisch vorgebar ist.

6. Vorrichtung nach Anspruch 5

dadurch gekennzeichnet, daß der fahrzeugspezifisch vorgebbare Abschnitt den Benutzercode (PIN) enthält.

7. Vorrichtung nach einem der vorhergehenden Ansprüche

dadurch gekennzeichnet, daß die Kopplung zwischen Steuereinrichtung (A) und Schlüsseleinrichtung (B) galvanisch, insbesondere in Form einer Chipkarte, erfolgt.

8. Vorrichtung nach einem der vorhergehenden Ansprüche

dadurch gekennzeichnet, daß die Kopplung zwischen Steuereinrichtung (A) und Schlüsseleinrichtung (B) kapazitiv und/oder induktiv erfolgt.

9. Verfahren zur Prüfung der Nutzungsberechtigung für Zugangskontrolleinrichtungen, insbesondere Schließeinrichtungen für Fahrzeuge, bei dem zwi-

schen einem zugangsseitigen, dauerenergieversorgten Steuergerät (A) und einer benutzerseitigen einen Transponder enthaltenden Schlüsseleinrichtung (B) bidirektional Identifikationsdaten ausgetauscht werden, wobei die Feststellung der für die Freigabe der Zugangseinrichtung erforderlichen Berechtigung derart erfolgt, daß eine vom Transponder (T) ausgesandte Codeinformation mit einer in der Steuereinrichtung (A) festgelegten Vorgabeinformation verglichen wird und daß nur bei einer Übereinstimmung eine Freigabe des Zugangs erfolgt

dadurch gekennzeichnet,

- a) daß zunächst die Schlüsseleinrichtung (B) an einen im Steuergerät (A) abgelegten geheimen Code (secret key) sowie einen Benutzercode (PIN) angelernt wird, und anschließend die vom Transponder (T) ausgesandte Information für den Vergleich mit der in der Steuereinrichtung (A) festgelegten Vorgabeinformation zur Feststellung der für die Freigabe der Zugangseinrichtung erforderlichen Berechtigung nach dem angelerntem geheimen Code verschlüsselt wird,
- b) und daß beim Ersetzen des Steuergerätes (A) durch ein weiteres Steuergerät (A') zunächst der Benutzercode (PIN) des ersten Steuergerätes (A) zur Schlüsseleinrichtung (B) übertragen wird, wodurch in der Schlüsseleinrichtung (B) nach Prüfung der Übereinstimmung des empfangenen Benutzercodes (PIN) mit dem angelerntem Benutzercode (PIN) der geheime Code mindestens teilweise zum Überschreiben freigegeben wird, und daß anschließend durch Übertragen des für das weitere Steuergerät (A') geltenden geheimen Codes (secret key') die Schlüsseleinrichtung (B) an den für das weitere Steuergerät (A') geltenden geheimen Code angelernt wird.

10. Verfahren nach Anspruch 9,

dadurch gekennzeichnet, daß die mindestens teilweise Freigabe des geheimen Codes in der Schlüsseleinrichtung nur dann erfolgt, wenn nicht eine vorgegebene Anzahl von Übertragungsvorgängen des Benutzercodes (PIN) überschritten worden ist.

50

55

